เอนก ศิรจริยาภิวัฒน์

หนทางต่อสู้และป้องกันไวรัส :
Stoned และ 1704

แนะนำวิธีตรวจเช็ค ไวรัสสโตนและ 1704 พร้อมลักษณะอาการที่เกิด

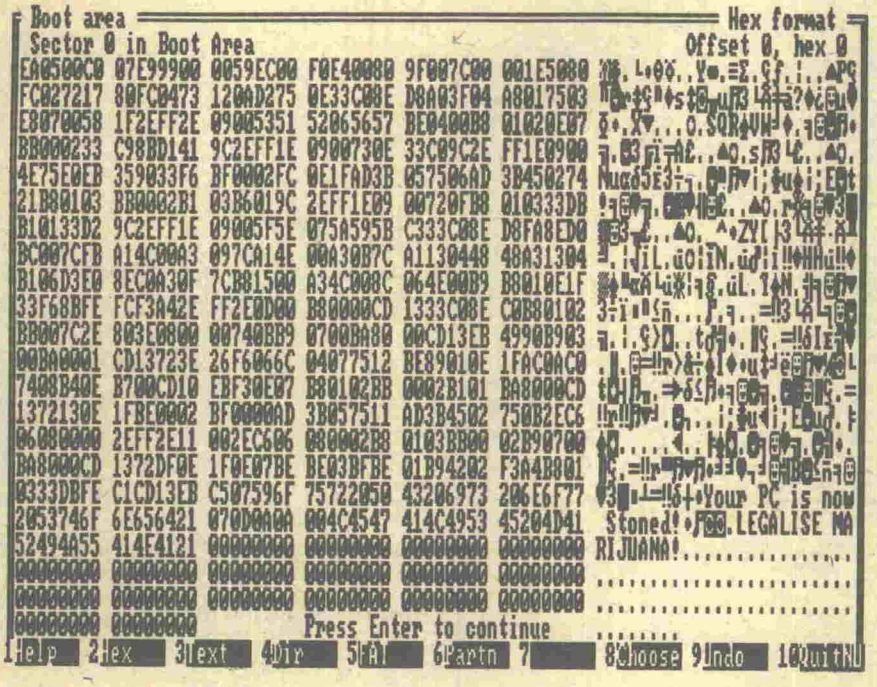
ตอนที่เริ่มบทความชุดนี้ ในใจของผมคิดว่าจะเขียนถึงเทคนิคและรายละเอียดของไวรัสแต่ละตัวให้มากที่สุด แต่เมื่อเห็นบทความเกี่ยวกับไวรัสหลาย ๆ บทความ ก็ทำให้เกิดอาการอยากเปลี่ยนใจขึ้นมาอย่างกะทันหัน สาเหตุเพราะยิ่งวิเคราะห์มากเท่าไรยิ่งทำให้เกิดความสับสน ทำให้ผู้อ่านส่วนใหญ่ที่เป็นผู้ใช้คอมพิวเตอร์ (ไม่ได้ทำงานด้านโปรแกรมเมอร์โดยตรง) ไม่อยากที่จะรับรู้อะไรมากขึ้น ซึ่งความคิดส่วนนี้เป็นความคิดของผมเองถ้าเป็นไปได้อยากให้ท่านผู้อ่านแสดงความคิดเห็นมาด้วย จะเป็นประโยชน์ต่อผู้อ่านท่านอื่น ๆ อีกมาก ขอขอบคุณล่วงหน้าครับ บทความคราวนี้จึงมีเฉพาะจุดสังเกตอาการและความเสียหายที่เกิดขึ้นเมื่อประสบกับ Stoned และ 1704 ไวรัส

Stoned ไวรัส

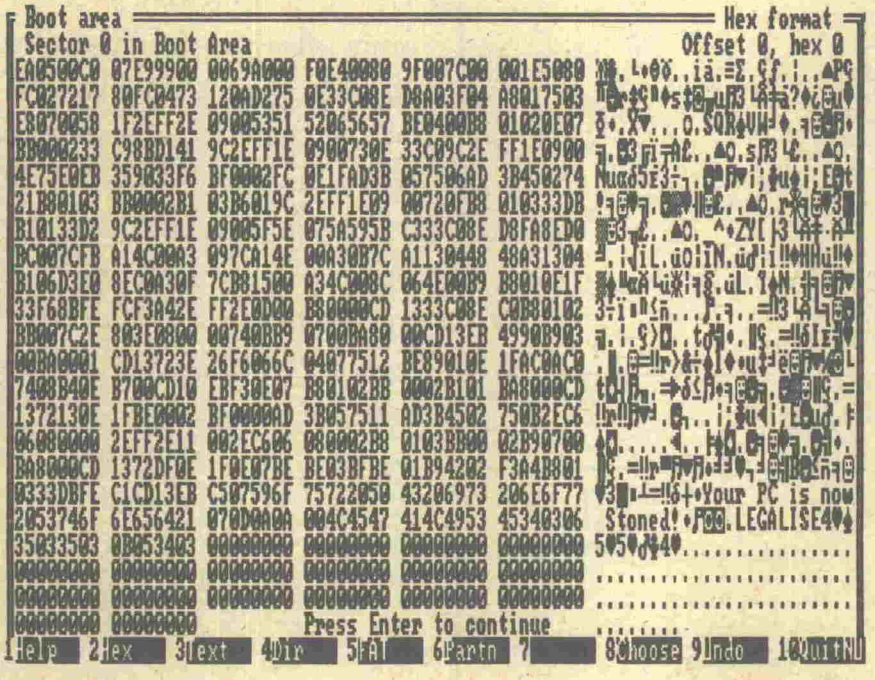
เมื่อพูดถึงไวรัสทีไร อดไม่ได้ที่จะต้องอ้างถึงโปรแกรมยูทิลิตี้ซึ่งจำเป็นต้องใช้ในการดูรายละเอียดของไวรัส โปรแกรมที่แนะนำคือนอร์ตันยูทิลิตี้และพีซีทูลส์อีกตัวที่ขาดแทบไม่ได้คือดีบัก ซึ่งวิธีการใช้ต้องขอให้ท่านผู้อ่านพยายามฝึกฝนกันเองนะครับ เรามาเริ่มสังเกตไวรัสสโตนกันเลยนะครับ

1. สิ่งแรกที่เกิดขึ้นก็คือ ไวรัสตัวนี้เป็นไวรัสประเภทบูตเรคอร์ด เมื่อเราใช้โปรแกรมดูบูตเรคอร์ดก็จะพบข้อความให้สังเกตตามรูปที่ 1 และ 2

2. เมื่อใช้โปรแกรมตรวจสอบหน่วยความจำ (เช่น MI ของพีซีทูลส์ หรือ SI ของนอร์ตันยูทิลิตี้) จะพบว่าหน่วยความจำของเครื่องหายไป 2K เมื่อพูดถึงเรื่องหน่วยความจำหายไปนี้ จึงอยากจะพูดถึงเครื่อง PS/2 สักหน่อยว่า ถ้าเกิดเราใช้โปรแกรมเช็คหน่วยความจำจะพบว่าหน่วยความจำจะหายไป 1K ซึ่งเป็นตัวเลขปกติของเครื่อง PS/2 นะครับ (โปรแกรมเช็คไวรัสบางตัว จะบอกว่ามีไวรัสเพราะโปรแกรมนั้นใช้วิธีเช็คจำนวนหน่วยความจำ) ความเสียหายที่เกิดขึ้นเรื่องนี้ไม่ค่อยพูดถึงกันซึ่งทำให้หลาย ๆ คนหวาดกลัวจนเกินเหตุหรือบางคนก็ไม่ระวังตัวจนเกินเหตุ (ไวรัสบางตัวอาการรุนแรงและสร้างความเสียหายมาก) สำหรับไวรัสสโตนนั้น หลาย ๆ คนไม่พบความเสียหายเลย สาเหตุเพราะไวรัสนี้จะมีผลเมื่อแผ่นดิสค์ของเรามีไฟล์ข้อมูลเกิน 96 ไฟล์ โดยไวรัสสโตนจะทำให้ชื่อไฟล์ที่ 97 ถึง 112 หายไป (ในกรณี



รูปที่ 1 Stoned II หรือ LEGALISE 4



รูปที่ 2 Stoned II หรือ MARIJUANA

ดิสค์แบบ DSDD) สาเหตุเพราะไวรัสสโตนจะย้ายส่วนบูตเรคอร์ดเดิมมาไว้ที่ส่วนท้ายของไดเรคทอรีจึงทำให้ชื่อไฟล์หายไป ส่วนของไวรัสสโตนผมคงกล่าวถึงเพียงแค่นี้ เพราะมีบทความเกี่ยวกับไวรัสตัวนี้หลายบทความแล้ว สำหรับวิธีแก้นั้นผมเองแนะนำให้ใช้โปรแกรม SCAN และ dean ของ Afree

1704

ไวรัสตัวนี้มีหลายเวอร์ชัน บางรุ่นอันตรายมาก (ดูข้อมูลได้จากบทความคราวก่อน) สำหรับตัวที่ผมมีอยู่คือรุ่น B และอีกตัวก็คือ Jo Jo ไวรัส ซึ่งก็คือไวรัส 1704 นั้นเอง (ดัดแปลงบางส่วนให้ทำงานทันทีเมื่อช่วงวันเวลาเป็นไปตามกำหนด) สำหรับอาการเกิดขึ้น

```
SI-System Information, Advanced Edition 4.50, (C) Copr 1987-88, Peter Norton

        Computer Name: IBM AT
     Operating System: DOS 3.30
  Built-in BIOS dated: Monday, June 13, 1988
       Main Processor: Intel 80386              Serial Ports: 2
        Co-Processor: None                     Parallel Ports: 2
Video Display Adapter: Monochrome (MDA)
   Current Video Mode: Text, 80 x 25 Monochrome
Available Disk Drives: 4, A: - D:

DOS reports 638 K-bytes of memory:
    54 K-bytes used by DOS and resident programs
   584 K-bytes available for application programs
A search for active memory finds:
   640 K-bytes main memory      (at hex 00000-0A000)
    64 K-bytes display memory   (at hex 0B000-0C000)
   384 K-bytes extended memory (at hex 10000-16000)
ROM-BIOS Extensions are found at hex paragraphs: C800 CB80

  Computing Index (CI), relative to IBM/XT: Testing...
      Disk Index (DI), relative to IBM/XT: Not computed. No drive specified.

Performance Index (PI), relative to IBM/XT: Not computed.
```

รูปที่ 3
ไวรัสสโตนทำให้หน่วยความจำหายไป 2 K

```
 Volume in drive A has no label
 Directory of  A:\

1             2             3             4             5
6             7             8             9             10
11            12            13            14            15
16            17            18            19            20
21            22            23            24            25
26            27            28            29            30
31            32            33            34            35
36            37            38            39            40
41            42            43            44            45
46            47            48            49            50
51            52            53            54            55
56            57            58            59            60
61            62            63            64            65
66            67            68            69            70
71            72            73            74            75
76            77            78            79            80
81            82            83            84            85
86            87            88            89            90
91            92            93            94            95
96            97            98            99            100
101           102           103           104           105
106           107           108           109           110
111           112
      112 File(s)     247808 bytes free
```

รูปที่ 4 รายชื่อไฟล์เมื่อไม่มีไวรัสสโตน (สร้างขึ้นมาเพื่อทดสอบ)

```
 Volume in drive A has no label
 Directory of  A:\

1             2             3             4             5
6             7             8             9             10
11            12            13            14            15
16            17            18            19            20
21            22            23            24            25
26            27            28            29            30
31            32            33            34            35
36            37            38            39            40
41            42            43            44            45
46            47            48            49            50
51            52            53            54            55
56            57            58            59            60
61            62            63            64            65
66            67            68            69            70
71            72            73            74            75
76            77            78            79            80
81            82            83            84            85
86            87            88            89            90
91            92            93            94            95
96            ô4ÊIBM    3.3
      97 File(s)     247808 bytes free
```

รูปที่ 5 รายชื่อไฟล์เมื่อแผ่นติดเชื้อไวรัสสโตน

นั้นท่านผู้อ่านที่มีไวรัสตัวนี้อยู่แล้วสามารถทดลองได้ แต่ขอให้เช็คให้แน่ใจว่าเป็นไวรัส 1704 รุ่น B เท่านั้น

1. ไวรัสตัวนี้เป็นแบบระดับไฟล์ไวรัส ซึ่งติดกับไฟล์นามสกุล .COM เท่านั้น (โดยไวรัสจะเช็คว่าข้อมูล 2 ตัวแรกเป็น 5A4D (บอกว่าไฟล์นั้นเป็นไฟล์ .EXE) หรือไม่ ขนาดของไฟล์จะเพิ่มขึ้น 1704 ไบต์

2. เมื่อใช้โปรแกรมเช็คการใช้หน่วยความจำของโปรแกรมต่าง ๆ จะพบว่ามีโปรแกรมประเภทฝังตัวเอง (TSR) ขนาด 688 ไบต์อยู่ในหน่วยความจำ ดังรูปที่ 6

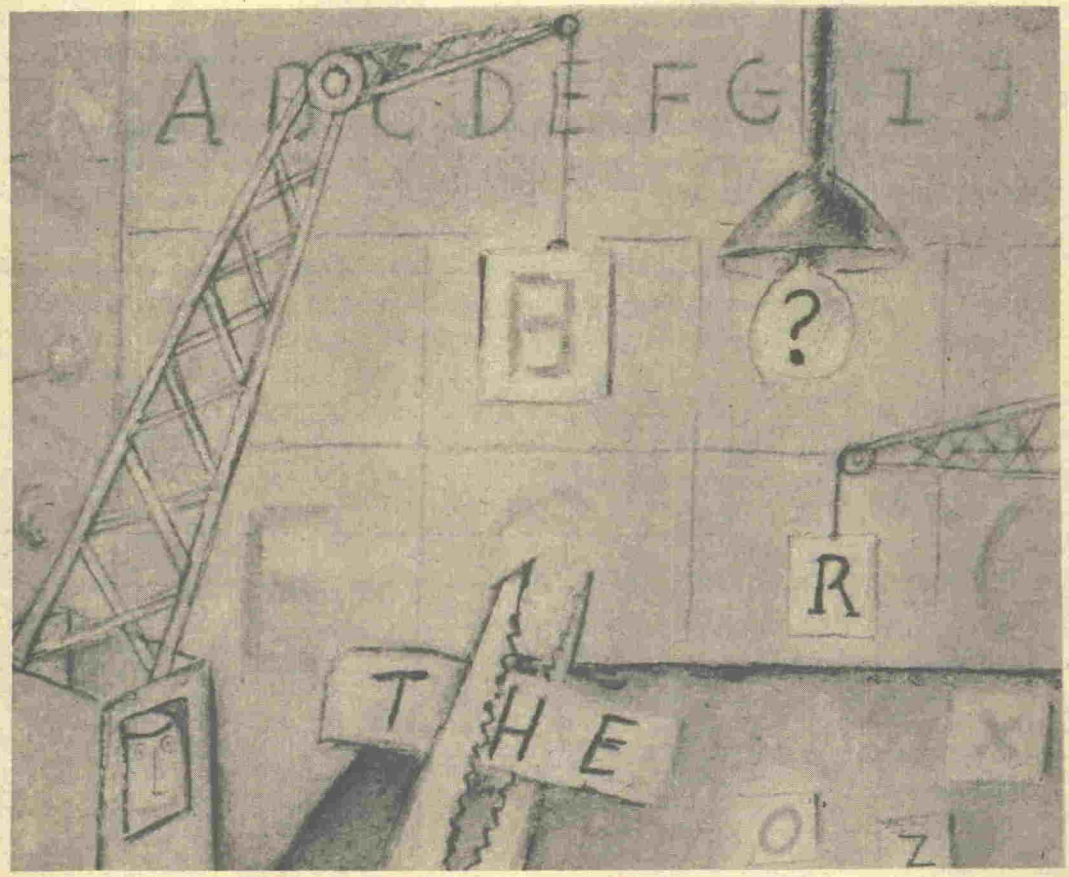
```
Allocated Memory Map - by TurboPower Software - Version 2.6

 PSP  blks bytes owner    command line        hooked vectors
----- ---- ----- -------- ------------------- ---------------------
0008    1   20400 config
0EC0    3    6144 command                     22 2E
0FF5    2    4000 NDE
10F3    1     688 N/A
119B    2  648784 free

block   bytes   (Expanded Memory)
-----   ------
    0  655360
 free  212992
total  868352
```

รูปที่ 6 ในหน่วยความจำมีโปรแกรมแปลกปลอมขนาด 688 ไบต์เมื่อ 1704 ไวรัสทำงาน

3. สำหรับอาการที่เกิดขึ้นนั้น ผมเองเอารูปมาลงให้ดูไม่ได้ เพราะเมื่อเกิดอาการแล้วเครื่องจะหยุดทำงานผมจึงขอเล่าเพียงอาการให้ฟังเท่านั้น อาการของไวรัสที่เกิดขึ้นถูกเรียกว่า falling character สาเหตุเพราะเมื่อตรงเงื่อนไขของไวรัสจะทำให้อักษรบางตัวตกลงมาอยู่ในบรรทัดด้านล่าง สมมติว่าในจอของเรามีคำว่า IBM Personal Computer DOS Version 3.30 เมื่อไวรัสแสดงอาการจะทำให้ตัวอักษรบางตัวหายไป (เพราะหล่นลงมาอยู่ด้านล่าง) ผมเองเอาตัวอย่างมาให้ดูดังรูปที่ 8 (ใช้โปรแกรมเวิร์ดโปรเซสซิงพิมพ์ให้เหมือนผลที่หน้าจอคอมพิวเตอร์)

4. ผลเสียหายก็คือ ขนาดของโปรแกรมเพิ่มขึ้นและบางครั้งเครื่องจะหยุดทำงาน โดยอาการจะเกิดขึ้นถ้าวันที่ของเครื่องอยู่ในช่วงเดือนตุลาคมถึงสิ้นปีของปี 1980 กับ 1988 เพราะฉะนั้นถ้าใครมี 1704 ไวรัสอยู่ก็สามารถทดลองได้ แต่อย่าลืมเช็ครุ่นของไวรัสก่อน สำหรับข้อ 1 นั้นจะเห็นว่าไฟล์ไวรัสจะมีการเพิ่มขนาดเป็นส่วนมาก (เท่าที่ทราบยังไม่มีตัวใดขนาดลดหรือขนาดเท่าเดิม) แต่การเพิ่มขนาดนี้บางครั้งเราสังเกตไม่ได้เพราะโปรแกรมนั้นอาจติดไวรัสไปแล้ว จึงสังเกตไม่ได้ มีวิธีตรวจง่าย ๆ ดังนี้ สมมติว่าสงสัยว่าโปรแกรมชื่อ MYPROG.COM (ชื่อสมมติ) ติดไวรัสหรือไม่ให้ทำตามนี้

```
A : \ DeBUG
     -A
     xxxx : 0100 MOV AX, 4C00
     xxxx : 0103 Int 21
     xxxx : 0105
```



```
-rcx
- CX 0000
:5
-ntest.com
-w
 Writing 0005 bytes
-Q
```

เมื่อเสร็จแล้วลองใช้คำสั่ง DIR Test.com ขนาดของ test.com จะเป็น 5 ไบต์ ลองทดสอบหน่วยความจำของเครื่องว่ามีไวรัสประเภทไฟล์อยู่หรือไม่ โดยทดลองให้โปรแกรม test.com ทำงานโดย

A: \ test

ทดลองใช้คำสั่ง DIR test.com อีกครั้ง ถ้าขนาดเพิ่มขึ้นแสดงว่าหน่วยความจำของเรามีไวรัสอยู่ เมื่อทดสอบหน่วยความจำว่าไม่มีไวรัสแล้ว ต่อไปทดสอบโปรแกรมว่ามีไวรัสอยู่หรือไม่ (สมมติโปรแกรมชื่อ MYPROG.COM)

A: \ VIRUS
A: \ test

ใช้คำสั่ง DIR test.com อีกครั้ง ดูว่าขนาดของ test.com เปลี่ยนไปหรือไม่ ถ้าเปลี่ยนแสดงว่า MYPROG.COM หวังว่าวิธีการเช็คนี้คงมีประโยชน์มากนะครับ

```
INTVIEW  Interrupt Viewer      Copyright (c) 1988,1989  V1.29  s/n U102241
 V COMMUNICATIONS, INC. · 3031 Tisch Way, Suite 802 · San Jose, CA  95128

Int  seg:off                 Comments                          Function
10  F000:F065  bios Award SoftwareIBM COMPATIBLE 28   Video I/O
11  F000:F84D  bios Award SoftwareIBM COMPATIBLE 28   Equipment check
12  F000:F841  bios Award SoftwareIBM COMPATIBLE 28   Memory size
13  0070:1DB1  dos  v3.30                             Disk I/O
14  F000:E739  bios Award SoftwareIBM COMPATIBLE 28   RS-232 I/O
15  09C4:03EB  dos  v3.30                             Special services
16  F000:E82E  bios Award SoftwareIBM COMPATIBLE 28   Keyboard I/O
17  F000:EFD2  bios Award SoftwareIBM COMPATIBLE 28   Printer I/O
18  F000:E3D4  bios Award SoftwareIBM COMPATIBLE 28   ROM Basic
19  0070:1920  dos  v3.30                             Bootstrap loader
1A  F000:FE6E  bios Award SoftwareIBM COMPATIBLE 28   Real time clock
1B  0070:0756  dos  v3.30                             Keyboard break
1C  10F4:06C0       141$FLu                           Timer break (18.2ms)
1D  F000:F0A4  ptr  (parameter table)                 Video table
1E  0000:0522  ptr  (parameter table)                 Disk table
1F  0000:0000  ptr  (parameter table)                 Graphic characters

PgUp, PgDn or 0-F for interrupt range      S-save to file      Esc to exit
```

```
INTVIEW  Interrupt Viewer      Copyright (c) 1988,1989  V1.29  s/n U102241
 V COMMUNICATIONS, INC. · 3031 Tisch Way, Suite 802 · San Jose, CA  95128

Int  seg:off                 Comments                          Function
20  0279:143F  dos  v3.30                             Program terminate
21  10F4:031F       141$FLu                           DOS general function
22  0EC0:012F  dos  v3.30                             Terminate address
23  0EC0:013C  dos  v3.30                             Ctrl-Break/Ctrl-C
24  0EC0:0556  dos  v3.30                             Critical error
25  0279:15DC  dos  v3.30                             Absolute disk read
26  0279:161F  dos  v3.30                             Absolute disk write
27  0279:6368  dos  v3.30                             Terminate & resident
28  10F4:0725       141$FLu                           Access often (undoc)
29  0070:069E  dos  v3.30                             Display char (undoc)
2A  0279:1445  dos  v3.30  iret                       NETBIOS services
2B  0279:1445  dos  v3.30  iret
2C  0279:1445  dos  v3.30  iret
2D  0279:1445  dos  v3.30  iret
2E  0EC0:0281  dos  v3.30                             Display chars(undoc)
2F  09C4:035D  dos  v3.30                             Multiplex & Spooler

PgUp, PgDn or 0-F for interrupt range      S-save to file      Esc to exit
```

รูปที่ 7 ใช้โปรแกรม INTVIEW ของ V communication จะพบว่าอินเตอร์รัพต์เบอร์ 1C, 21 และ 28 มีอักษรว่า 141$FLU แต่ INTVIEW ก็ติดไวรัสไปแล้ว

```
IBM Person l Comput r Dos VerS on 3

c:\>a
     :    a        e          i    .30
a:\>1704

a:\>

Internal Stack overflow
System halted
```

รูปที่ 8 อาการของ 1704 ไวรัส